UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/976,447	10/12/2001	Takayuki Sato	04610.004001	3936

22511 7590 02/08/2006

OSHA LIANG L.L.P.
1221 MCKINNEY STREET
SUITE 2800
HOUSTON, TX 77010

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 02/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/976,447	SATO, TAKAYUKI	
	Examiner	Art Unit	
	Benjamin E. Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5,11-14,16,20 and 26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5,11-14,16,20 and 26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 October 2001* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 22 December 2005 amend claims 1, 11-14, 16, and cancels claims 2-4, 6-10, 15, 17-19, 21-25, and 27-34. Applicant's amendment has been fully considered and is entered.

Response to Arguments

2. Applicant's arguments filed 22 December 2005 have been fully considered but they are not persuasive. Applicant's argument that Kalajan does not disclose an intelligent interconnecting device connected to a LAN trunk line..." is not persuasive because Figure 1 of Kalajan shows the firewall connected to a LAN line network for protection of a network resource (Abstract).

3. Applicant's contention that Kalajan discloses avoiding the receipt of unauthorized packets, wherein the present invention is aimed towards avoiding unauthorized access to an intelligent interconnecting device which depends on TCP/IP protocol is not persuasive because the destination server firewall is configured for access control over a network resource (Abstract) over the Internet (Col. 1, lines 17-19 & Col. 3, lines 49-51, 55-56). Use of the TCP/IP protocol is inherent to Internet communications.

4. Applicant's argument that Kalajan fails to show the determination of a first access, and that the validation of Kalajan must occur at every access is not persuasive because Kalajan shows that at the time of the client access to the network resource, which is an access-controlled port, that no communication path has been established (Col. 3, line 64 – Col. 4, line 1). This is an example of a first access of a particular session, which would meet the limitation of a first

access. Once validated, the client packets directed to the access-controlled port, would be filtered and accepted at the firewall because the client's source IP address would be recognized. This would meet the limitations of "...permitting communication thereafter..." This rationale also applies to Applicant's arguments with respect to claims 11, 12, 14, and 16.

5. Applicant's argument that Kalajan only provides access to a port is not persuasive because the client is being granted access to the server through the access-controlled port. The public can only access the publicly accessibly port and cannot access stored information within the server. Only when validated can the client gain access to the information stored in the server through the access-controlled port (Figure 1 & Col. 4, lines 33-65). A server would meet the limitation of an intelligent interconnecting device.

6. Applicant's argument with respect to the amended claim limitations of claim 1 that came from previous claim 2 is not persuasive because claim 2 was rejected over Kalajan, in view of Barrett. Therefore, the previous rejection of claim 2 will now be applicable to amended claim 1.

7. Applicant's argument that the Barrett reference does not disclose, "notifying an authenticated managing computer..." is not persuasive because Barrett discloses building the list of blocked source IP addresses. Therefore, the server that stores the blocked source IP address list would be notified when a new IP address needs to be added. This rationale also applies to Applicant's arguments with respect to claims 13 and 16.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

10. Claim 1 defines "an external apparatus" multiple times, which renders the claim vague and indefinite because it is unclear whether each recitation is intended to be the same external apparatus or whether they are intended to different external apparatuses.

11. Claim 1 recites, "judging, when an access from an external apparatus occurs thereafter..." which renders the claims vague and indefinite because the claim previously claims a judging procedure that determines whether an attempted access from an external apparatus has been made. Therefore, it is unclear whether this judging procedure is meant to determine a second access or whether this judging procedure is determining the same access as claimed previously.

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. Claims 11, 12, 14 are rejected under 35 U.S.C. 102(e) as being anticipated by Kalajan, U.S. Patent No. 6,205,156. Referring to claim 11, Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56), which meets the limitation of packets being

transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol. In order to establish the communication path the first client must validate itself to the server using a one-time password (Col. 3, line 64 – Col. 4, line 4), which meets the limitation of a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred, a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred, a third step of causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not authentication is given, a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given. Once the first client is validated, the IP address (Col. 3, lines 50-51) of the first client is considered a validated network address by the server and the client validation system of the server establishes the access-controlled communications path by instructing firewall to allow packets from the first client (Col. 4, lines 22-31), which meets the limitation of a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from an external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in said fourth step. If the client is not authenticated the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter

by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in said third step. During communications over the access-controlled communications path, the firewall allows only data packets from validated network addresses to pass through to access-controlled port. Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41), which meets the limitation of a seventh step of causing the intelligent interconnecting device to judge whether or not a source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in said first step, an eighth step of determining the external apparatus whose source IP address is judged to be identical with the stored source IP address as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to process the steps beginning from said second step, when the source IP address of the external apparatus is judged to be identical with the stored source IP address in said seventh step. If the client network address does not match then the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a ninth step of determining the external apparatus whose source IP address is judged to be nonidentical with the stored source IP address as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in said seventh step. Figure 1 of Kalajan shows the firewall connected to a LAN line network for protection of a network resource (Abstract), which meets the limitation of a LAN trunk line.

Referring to claims 12, 14, Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56), which meets the limitation of a LAN trunk link interfacing section having an interface function with a LAN trunk line, packets being transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol. In order to establish the communication path the first client must validate itself to the server using a one-time password (Col. 3, line 64 – Col. 4, line 4), which meets the limitation of a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred, a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred, a third step of causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not authentication is given, a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given. Once the first client is validated, the IP address (Col. 3, lines 50-51) of the first client is considered a validated network address by the server and the client validation system of the server establishes the access-controlled communications path by instructing firewall to allow packets from the first client (Col. 4, lines 22-31), which meets the limitation of a storage section for storing a program and data therein, a fifth step of causing the intelligent interconnecting device to extract and store a

source IP address included in a packet which is received from an external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in said fourth step. If the client is not authenticated the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in said third step. During communications over the access-controlled communications path, the firewall allows only data packets from validated network addresses to pass through to access-controlled port, which meets the limitation of a port interfacing section having an interface function with a terminal connected thereto. Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41), which meets the limitation of a central controlling section for controlling operations of said LAN trunk line interfacing section, said port interfacing section, and said storage section, a seventh step of causing the intelligent interconnecting device to judge whether or not a source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in said first step. The communication path is maintained between the client and the server for a predetermined period of time. The communication path is terminating at the end of the period of time and the client must be revalidated to resume the access-controlled communication path (Col. 4, line 66 – Col. 5, line 10), which meets the limitation of an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined

valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in said seventh step, an ninth step of determining the external apparatus whose source IP address is judged to be the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from said second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in said eighth step. If the client network address does not match then the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a tenth step of determining the external apparatus whose source IP address is judged to be nonidentical or is judged to be no within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in said seventh step or is judged to be not within the predetermined valid period in said eighth step. While Kalajan discloses that if a connection with a client is blocked, no information regarding the blocking of the connection will be sent to the client, the teaching still meets the limitation of notifying an authenticated managing computer of the source IP address of the external apparatus which is judged to be nonidentical when the source IP address is judged to be nonidentical with the stored source IP address for the same reasoning mentioned above. Figure 1 of Kalajan shows the firewall connected to a LAN line network for protection of a network resource (Abstract), which meets the limitation of a LAN trunk line.

Claim Rejections - 35 USC § 103

14. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

16. Claims 1, 5, 13, 16, 20, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kalajan, U.S. Patent No. 6,205,156, in view of Barrett, U.S. Patent No. 6,832,321. Referring to claim 1, Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56), which meets the limitation of packets being transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol. In order to establish the communication path the first client must validate itself to the server using a form of one-time validation (Col. 3, line 64 – Col. 4, line 4). Once the first client is validated, the IP address (Col. 3, lines 50-51) of the first client is considered a validated network address by the server and the client validation system of the server establishes the access-controlled communications path by instructing firewall to allow packets from the first client (Col. 4, lines 22-31), which meets the limitation of extracting and storing a source IP

address included in a packet which is transmitted from an external apparatus when an access from the external apparatus is authenticated through execution of the TCP/IP protocol. During communications over the access-controlled communications path, the firewall allows only data packets from validated network addresses to pass through to access-controlled port. Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41), which meets the limitation of judging when an access from an external apparatus occurs thereafter, whether or not a source IP address of the external apparatus giving the access is identical with the stored source IP address, permitting communication thereafter between the external apparatus having the source IP address identical with the stored transmitting end IP address and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be identical with the stored source IP address. Figure 1 of Kalajan shows the firewall connected to a LAN line network for protection of a network resource (Abstract), which meets the limitation of a LAN trunk line. Kalajan shows that at the time of the client access to the network resource, which is an access-controlled port, that no communication path has been established (Col. 3, line 64 – Col. 4, line 1). This is an example of a first access of a particular session, which would meet the limitation of a first access. Once validated, the client packets directed to the access-controlled port, would be filtered and accepted at the firewall because the client's source IP address would be recognized. This would meet the limitations of "...permitting communication thereafter..." Kalajan does not disclose that the server contains a list of block source IP addresses. Barrett discloses a network access server

having a firewall wherein the access server maintains a list of allowed IP addresses and blocked IP addresses (Col. 9, lines 32-37). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a list of blocked IP address is the access control system of Kalajan in order to specify that inbound connections with certain source addresses should be blocked as taught in Barrett (Col. 9, lines 51-54).

Referring to claim 5, Kalajan discloses that the communication path is maintained between the client and the server for a predetermined period of time. The communication path is terminating at the end of the period of time and the client must be revalidated to resume the access-controlled communication path (Col. 4, line 66 – Col. 5, line 10), which meets the limitation of judging whether or not the source IP address which is judged to be identical with the stored source IP address is within a valid period set in advance when the source IP address is judged to be identical with the stored source IP address, permitting communication thereafter between the external apparatus having the source IP address which is judged to be within the valid period and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be within the valid period.

Referring to claim 13, Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56), which meets the limitation of a LAN trunk line interfacing section having an interface function with a LAN trunk line, packets being transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol. In order to establish the communication path the first client must validate itself to the server using a one-time password (Col. 3, line 64 – Col. 4, line 4), which

meets the limitation of a first step of causing the intelligent interconnecting device to judge whether or not a first access to the intelligent interconnecting device from outside has occurred, a second step of causing the intelligent interconnecting device to carry out authentication processing by using a user identifier and a password based on the TCP/IP protocol when it is judged in said first step that the first access from outside has occurred, a third step of causing the intelligent interconnecting device to judge after the authentication processing in said second step whether or not authentication is given, a fourth step of determining an authenticated external apparatus as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to judge whether or not this access is the first access, when it is judged in said third step that the authentication is given. Once the first client is validated, the IP address (Col. 3, lines 50-51) of the first client is considered a validated network address by the server and the client validation system of the server establishes the access-controlled communications path by instructing firewall to allow packets from the first client (Col. 4, lines 22-31), which meets the limitation of a storage section for storing a program and data therein, a fifth step of causing the intelligent interconnecting device to extract and store a source IP address included in a packet which is received from an external apparatus in the authentication processing when this access of the external apparatus is judged to be the first access in said fourth step. If the client is not authenticated the client is not responded to (Col. 4, lines 46-50), which meets the limitation of a sixth step of determining the external apparatus as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the external apparatus is judged not to be authenticated in said third step. During communications over the access-controlled communications path, the firewall allows only data packets from

validated network addresses to pass through to access-controlled port, which meets the limitation of a port interfacing section having an interface function with a terminal connected thereto. Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41), which meets the limitation of a central controlling section for controlling operations of said LAN trunk line interfacing section, said port interfacing section, and said storage section, a seventh step of causing the intelligent interconnecting device to judge whether or not a source IP address of the external apparatus giving the access thereto is identical with the stored source IP address when this access is judged not to be the first access in said first step. The communication path is maintained between the client and the server for a predetermined period of time. The communication path is terminating at the end of the period of time and the client must be revalidated to resume the access-controlled communication path (Col. 4, line 66 – Col. 5, line 10), which meets the limitation of an eighth step of causing the intelligent interconnecting device to judge whether or not the source IP address is within a predetermined valid period when the source IP address of the external apparatus is judged to be identical with the stored source IP address in said seventh step, an ninth step of determining the external apparatus whose source IP address is judged to be the predetermined valid period as an apparatus to be responded to thereafter by the intelligent interconnecting device and causing the intelligent interconnecting device to execute the steps beginning from said second step, when the source IP address of the external apparatus is judged to be within the predetermined valid period in said eighth step. If the client network address does not match then the client is not responded to (Col.

4, lines 46-50), which meets the limitation of a tenth step of determining the external apparatus whose source IP address is judged to be nonidentical or is judged to be no within the predetermined valid period as an apparatus not to be responded to thereafter by the intelligent interconnecting device when the source IP address of the external apparatus is judged to be nonidentical with the stored source IP address in said seventh step or is judged to be not within the predetermined valid period in said eighth step. While Kalajan discloses that if a connection with a client is blocked, no information regarding the blocking of the connection will be sent to the client, the teaching still meets the limitation of notifying an authenticated managing computer of the source IP address of the external apparatus which is judged to be nonidentical when the source IP address is judged to be nonidentical with the stored source IP address for the same reasoning mentioned above. Figure 1 of Kalajan shows the firewall connected to a LAN line network for protection of a network resource (Abstract), which meets the limitation of a LAN trunk line. Kalajan does not disclose that the server contains a list of block source IP addresses. Barrett discloses a network access server having a firewall wherein the access server maintains a list of allowed IP addresses and blocked IP addresses (Col. 9, lines 32-37). It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a list of blocked IP address is the access control system of Kalajan in order to specify that inbound connections with certain source addresses should be blocked as taught in Barrett (Col. 9, lines 51-54). Applicant's argument that the Barrett reference does not disclose "notifying an authenticated managing computer..." is not persuasive because Barrett discloses building the list of blocked source IP addresses. Therefore, the server that stores the blocked source IP address list would be notified when a new IP address needs to be added.

Referring to claims 16, 26, Kalajan discloses an access control system wherein a communication data path is established between a first client and a HTTP server over the Internet (Col. 3, lines 43-45, 55-56), which meets the limitation of a LAN trunk line interfacing section having an interface function with a LAN trunk line, packets being transmitted/received between a plurality of computers and being structured to be controllable by an external apparatus based on a TCP/IP protocol. In order to establish the communication path the first client must validate itself to the server using a form of one-time validation (Col. 3, line 64 – Col. 4, line 4). Once the first client is validated, the IP address (Col. 3, lines 50-51) of the first client is considered a validated network address by the server and the client validation system of the server establishes the access-controlled communications path by instructing firewall to allow packets from the first client (Col. 4, lines 22-31), which meets the limitation of a storage section for storing a program and data therein, extracting and storing a source IP address included in a packet which is transmitted from an external apparatus and stored in said storage section when an access from the external apparatus is authenticated through execution of the TCP/IP protocol. During communications over the access-controlled communications path, the firewall allows only data packets from validated network addresses to pass through to access-controlled port, which meets the limitation of a port interfacing section having an interface function with a terminal connected thereto. Each communications or data packet from a client typically includes information indicating the source network address of the packet. This information can be used to determine whether or not the server will accept the packets or communicate with the source of incoming communications (Col. 4, lines 33-41), which meets the limitation of a central controlling section for controlling operations of said LAN trunk line interfacing section, said port

interfacing section and said storage section, judging when an access from an external apparatus occurs thereafter, whether or not a source IP address of the external apparatus giving the access is identical with the stored source IP address, permitting communication thereafter between the external apparatus having the source IP address identical with the stored transmitting end IP address and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be identical with the stored source IP address. Figure 1 of Kalajan shows the firewall connected to a LAN line network for protection of a network resource (Abstract), which meets the limitation of a LAN trunk line. Kalajan does not disclose that the server contains a list of block source IP addresses. Barrett discloses a network access server having a firewall wherein the access server maintains a list of allowed IP addresses and blocked IP addresses (Col. 9, lines 32-37), which meets the limitation of when the source IP address is judged to be nonidentical with the stored source IP address, said central controlling section registers the source IP address which is judged to be nonidentical with the stored source IP address in an unauthorized access IP list. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a list of blocked IP address is the access control system of Kalajan in order to specify that inbound connections with certain source addresses should be blocked as taught in Barrett (Col. 9, lines 51-54). Applicant's argument that the Barrett reference does not disclose "notifying an authenticated managing computer..." is not persuasive because Barrett discloses building the list of blocked source IP addresses. Therefore, the server that stores the blocked source IP address list would be notified when a new IP address needs to be added.

Referring to claim 20, Kalajan discloses that the communication path is maintained between the client and the server for a predetermined period of time. The communication path is terminating at the end of the period of time and the client must be revalidated to resume the access-controlled communication path (Col. 4, line 66 – Col. 5, line 10), which meets the limitation of judging whether or not the source IP address which is judged to be identical with the stored source IP address is within a valid period set in advance when the source IP address is judged to be identical with the stored source IP address, permitting communication thereafter between the external apparatus having the source IP address which is judged to be within the valid period and the intelligent interconnecting device only when the source IP address of the external apparatus is judged to be within the valid period.

Conclusion

17. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100